



300-720^{Q&As}

Securing Email with Cisco Email Security Appliance (SESA)

Pass Cisco 300-720 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/300-720.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

Refer to the exhibit.



Edit Incoming Content Filter

Content Filter Settings

Name:	exe
Currently Used by Policies:	marketing_team
Description:	Scans for executable attachments as a standalone, renamed to a different extension or hidden inside archives.
Order:	1 (of 12)

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	Attachment File Info	attachment-filetype == "Executable"	

Actions

Add Action...

Order	Action	Rule	Delete
Final	Drop (Final Action)	drop ()	

Scan Behavior

Attachment Type Mappings

Add Mapping...		Import List...	
Fingerprint / MIME	Type	Edit	Delete
Fingerprint	Image		
Fingerprint	Media		
MIME Type	audio/*		
MIME Type	video/*		
Export List...			

Global Settings

Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	1
Maximum attachment size to scan:	SM
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

```
Tue Aug 13 17:39:51 2019 Info: New SMTP ICID 391975 interface Management (10.66.71.122) address 10.137.84.196 reverse
dns host unknown verified no
Tue Aug 13 17:39:51 2019 Info: ICID 391975 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918 country not
applicable
Tue Aug 13 17:39:51 2019 Info: Start MID 379145 ICID 391975
Tue Aug 13 17:39:51 2019 Info: MID 379145 ICID 391975 From: <matt@lee.com>
Tue Aug 13 17:39:51 2019 Info: MID 379145 ICID 391975 RID 0 To: <bob_doe@cisco.com>
Tue Aug 13 17:39:54 2019 Info: MID 379145 Message-ID '<op.z6f4nirfuxysu2@mathuynh-f645d.mshome.net>'
Tue Aug 13 17:39:54 2019 Info: MID 379145 Subject 'IMPORTANT ATTACHMENT PLEASE OPEN'
Tue Aug 13 17:39:55 2019 Info: MID 379145 ready 3917905 bytes from <matt@lee.com>
Tue Aug 13 17:39:55 2019 Info: MID 379145 matched all recipients for per-recipient policy marketing_team in the inbound table
Tue Aug 13 17:39:55 2019 Info: ICID 391975 close
Tue Aug 13 17:39:55 2019 Info: graymail [RPC_CLIENT] Graymail scan skipped since message size exceeds configured
threshold
Tue Aug 13 17:39:55 2019 Info: MID 379145 was too big (3917905/524288) for scanning by Outbreak Filters
Tue Aug 13 17:39:55 2019 Info: MID 379145 was too big (3917905/2097152) for scanning by CASE
Tue Aug 13 17:39:57 2019 Info: MID 379145 using engine: GRAYMAIL negative
Tue Aug 13 17:39:57 2019 Info: MID 379145 attachment 'dangerous_file.zip'
Tue Aug 13 17:39:57 2019 Warning: MID 379145, Message Scanning Problem: Scan Depth Exceeded
Tue Aug 13 17:39:57 2019 Info: MID 379145 queued for delivery
```



Which configuration allows the Cisco ESA to scan for executables inside the zip and apply the action as per the content filter?

- A. Modify the content filter to look for .exe filename instead of executable filetype.
- B. Configure the recursion depth to a higher value.
- C. Configure the maximum attachment size to a higher value.
- D. Modify the content filter to look for attachment filetype of compressed.

Correct Answer: C

QUESTION 2

A Cisco ESA administrator has several mail policies configured. While testing policy match using a specific sender, the email was not matching the expected policy.

What is the reason of this?

- A. The "From" header is checked against all policies in a top-down fashion.
- B. The message header with the highest priority is checked against each policy in a top-down fashion.
- C. The "To" header is checked against all policies in a top-down fashion.
- D. The message header with the highest priority is checked against the Default policy in a top-down fashion.

Correct Answer: D

QUESTION 3

A Cisco ESA administrator recently enabled the Outbreak Filters Global Service Setting to detect Viral as well as Non-Viral threat detection, with no detection of Non-Viral threats after 24 hours of monitoring Outbreak Filters. What is the reason that Non-Viral threat detection is not detecting any positive verdicts?

- A. The Outbreak Filters option Graymail Header must be enabled.
- B. The Outbreak Filters option URL Rewriting must be enabled.
- C. Non-Viral threat detection requires AntiSpam or Intelligent Multi-Scan enablement to properly function.
- D. Non-Viral threat detection requires AntiVirus or AMP enablement to properly function.

Correct Answer: C

QUESTION 4

Which two components form the graymail management solution in Cisco ESA? (Choose two.)

- A. cloud-based unsubscribe service



- B. uniform unsubscription management interface for end users
- C. secure subscribe option for end users
- D. integrated graymail scanning engine
- E. improved mail efficacy

Correct Answer: AD

Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01101.pdf (p.2)

QUESTION 5

When outbreak filters are configured, which two actions are used to protect users from outbreaks? (Choose two.)

- A. redirect
- B. return
- C. drop
- D. delay
- E. abandon

Correct Answer: AD

Reference: https://www.cisco.com/c/en/us/td/docs/security/esa/esa12-0/user_guide/b_ESA_Admin_Guide_12_0/b_ESA_Admin_Guide_chapter_01110.html

[300-720 PDF Dumps](#)

[300-720 Practice Test](#)

[300-720 Study Guide](#)